information. It defines a data structure including location information, security requirements, policy mechanism and entities involved forming a complete architecture. Included in the requirements for exchanging the SLO structure among entities, is a need for a transport means, which must be scalable and secure. In this invention SIP used as the transport protocol for the SLO data fulfills these requirements.

[**0072**] The invention shows how to effect a common service for providing the user location following the SLO structure, using the SIP as the transport mechanism. Disclosed herein is how the SIP entities fit in the SLO architecture requirements while providing all the requisites needed by the SLO definition. Basically, the invention shows how SLO and SIP may be complemented to perform a global user location service.

[**0073**] The SIP protocol and all the entities involved in a SIP session are known from RFC 2543 but will be briefly described below. Also described are the SIP messages and the mechanisms provided by SIP for Addressing and performing user mobility. Next to be described below is the SLO, where the requirements for defining a common architecture for providing the SLO data over IP networks are explained. The SLO structure and the different parts of the message adopted for providing a complete location information are described. Third, how both the SIP and SLO architectures fit together is illustrated, the former as the transport means for the latter. The SLO requirements are described in the context of the existing SIP functionalities. Finally, some basic scenarios of how SIP and SLO will behave together in a normal transaction are shown.

[**0074**] SIP Introduction

[**0075**] The Session Initiation Protocol (SIP) is an application-layer control protocol that can establish, modify and terminate multimedia sessions or calls. SIP is text-based, using ISO 10646 in UTF-8 encoding throughout. This makes SIP flexible and extensible and since it use for initiating multimedia conferences rather than delivering data, the overhead for using text-based is not significant. The syntax of the messages is similar to HTTP but SIP instead can carry the transaction using either UDP or TCP. The message can be either a Request or Response and it is created following the format of D. Crocker, "Standard for the format of ARPA Internet text messages," RFC 822, IETF, August 1982.

[**0076**] SIP Entities

[**0077**] The entities involved in a SIP session are the User Agent, the Proxy server, Redirect server, Registrar server and the Location server.

[**0078**] The User Agent (UA) can act like a client (UAC) that is a client application that initiates a SIP request. The User Agent can also act like a server (UAS) that is a server application that contacts the user when a SIP request is received and send back a response on behalf of the user.

[**0079**] The Proxy server is an intermediate entity that behaves like client and server simultaneously. It can interpret and modify the request before forwarding it to other servers.

[**0080**] The Redirect server is an entity that receives the request and maps the address to which the message was initially directed into zero or more new addresses. Then, the client should try again using the new addresses returned from the Redirect server to contact the caller or another SIP server that can handle the message in case of special requirements.

[**0081**] The Registrar server is a server that accepts the user registration (REGISTER message) and can make this information available through the location server The Location server is an element used by a Redirect or Proxy server to obtain information about the possible location of the callee. It can include Registrar server or any mobility registration protocol available for this purpose.

[**0082**] Message Structure

[**0083**] The message consists of a start line, one or more header fields, an empty line (Carriage-return line-feed, CRLF) and an optional body. Three examples are shown in **FIGS. 2, 3** and **4**.

[**0084**] Basically, the start line indicates if it is a Request (INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER, etc.) or a Response (100 Informational, 200 Success, 300 Redirection, 400 Client Error, 500 Server Error or 600 Global Failure).

[**0085**] The message header is composed by multiple headers indicating, the Origin ("From: "), Destination ("To:"), Call Identifier ("Call-ID:"), Message Sequence ("Cseq: "), Transaction path ("Via:"), the length ("Content-Length:") and content ("Content-Type:") of the body if it carried in the message.

[**0086**] Finally, the message body can contain any kind of data and its interpretation depends of the type of message. Generally the content of the body can contain a session description following a specific format such as the Session Description Protocol (SDP), text or XML scripts. The "Content-Type" header field gives the media type of the message body. If the body has concrete encoding it is indicated in the "Content-Encoding" header field. The body length is given in the "Content-Length" header field.

[**0087**] SIP Addressing

[**0088**] The entities addressed by SIP are user at hosts and they are identified by a SIP URL, see T. Berners-Lee, R. Fielding and L. Masinter, "Uniform resource Locators (URL)," RFC 1738, IETF, December 1994. The URL takes a form such as user@host where the user part can be a user name or telephone number and the host would be either a domain name or a network address. The SIP URLs are used within the SIP messages to indicate the originator (From), the current destination in the start line (Request URL) and the final recipient (To) of a SIP request. Its interpretation follows the guidelines of RFC 2396 "Uniform resource identifier (UR1)," IETF, August 1998, by T. Berners-Lee et al. and the syntax is described using Augmented Backus-Naur form, using characters reserved within any given URI component.

[**0089**] The SIP URL is used for locating a user based on DNS SRV lookup. The client queries the DNS server including for address records for the destination address. If the DNS does not return any address record, it means that the end user cannot be located. Other alternative protocols for locating a user are finger (RFC 1288 D. Zimmerman, "The finger user information protocol," RFC 1288, IETF, December 1991), rwhois (RFC 2167 S. Williamson, et al. "Referral